

Data Processing Agreement — Cybersol B.V. / OBLIGO

Interim revision v14.2.1 — 5 October 2026 — issued 5 October 2026 (the date this PDF was built). v14.2.1 corrects one statement in v14.2 and is a non-material revision under section 9.4(b): section 9.1 no longer describes the Dutch-law formation basis for online acceptance as an open review point; it records counsel's advice of 14 August 2026 on that point and the four evidence safeguards counsel recommended, and states that this advice is not proof that the acceptance mechanism meets them. No other text changes. The PDF of this revision was generated on 5 October 2026 from this text.

*Interim revision v14.2 — 5 October 2026 — issued 5 October 2026 (the date this PDF was built). v14.2 aligns v14.1 with the OBLIGO Terms of Service. It is a user-facing revision, not a version sent to counsel, and it is a **material revision under section 9.4**: (i) the Parties section and sections 9.2 and 9.5 identify the Customer as the legal entity identified as the Customer under the Agreement, and require whoever accepts online or signs a written instrument to confirm their authority; (ii) sections 8.2 and 8.3 name the OBLIGO Terms of Service as the home of the liability cap, operative only while a version of those Terms is validly in force and incorporated in the Agreement, and section 8.2 states that the cap also applies to claims between the Parties for recourse or indemnity relating to compensation paid under Article 82 GDPR, to the extent mandatory law allows, and section 8.3 records counsel's view on that point and the legal questions that remain open; (iii) section 4(g) states the audit-record retention that Annex 1 already referred to, with its open item; (iv) section 9.1 places electronic acceptance at the Customer's first access to the Services after approval of its application, and in any case before normal use; (v) the Annex 2 no-training row attributes counsel's answer to the addendum; (vi) the Annex 2 abuse-monitoring row changes only once a changed arrangement is in effect and verified, and states the arrangement as verified on the date it gives; (vii) the Annex 3 contractor row records a correction the engineer made on 4 October 2026; (viii) section 4(g), the Annex 1 Duration row and the Annex 2 Backups row state, alongside the 30-to-35-day lifecycle deletion of backup copies, the further 30-day soft-delete period during which a deleted copy remains recoverable. Sections 5.3, 6.3 and 6.4 are unchanged. These changes will be carried into the next consolidated version for counsel; the legal points they touch remain open for that review. The PDF of this revision was generated on 5 October 2026 from this text.*

Interim revision v14.1 — 9 September 2026 — issued 10 September 2026 (the date this PDF was built). v14.1 is a user-facing correction of v14, not a version sent to counsel: (i) the abuse-monitoring row's status is corrected — the modified-abuse-monitoring application was submitted on 25 August 2026 and refused by the vendor on 27 August 2026, so the vendor default described in that row remains in effect; the retention-limitation wording is unchanged; (ii) section 6.1 now states how the outside-EEA access is classified, on counsel's advice received in September 2026, and the status of the written contract and transfer mechanism for it as at 9 September 2026; (iii) Annex 3 gains a row for the individual contractor concerned; (iv) the no-training row records counsel's answer to the question v10 reserved; (v) section 6.4 records a transitional commitment. Sections 5.3 and 6.3 are unchanged: the disclosures in this revision qualify no undertaking. The changes will be carried into the next consolidated version for counsel. The PDF of this revision was generated on 10 September 2026 from this text.

Internal working revision v14 — 24 August 2026 — sent to counsel on 25 August 2026 and confirmed, against the comparison document, in counsel's response of September 2026. (This header was written before the send and said "not sent"; corrected in v14.1 with the chain preserved.) **v14 changes one thing and it is not substance**: two sentences, at §6.1 and §10, identified the deployed production build by its internal version-control identifier. That identifier means nothing to a reader outside Cybersol and does not belong in an external document, so both now refer to the sealed release by the date it was verified. Every fact either sentence carried is unchanged — the sealed-release mechanism, the dates of the changes it contains, and what follows from them. Otherwise v14 is v13, whose own summary follows. Counsel held **v10, sent 9 August 2026** (the 10 August date on that file is its document date, not the send date) until this*

v14 was sent on 25 August 2026; **v11 of 10 August 2026 and v12 of 17 August 2026 were never sent either.** This v13 is the consolidated revision made after counsel's advice part 2: it carries counsel's answered wording where the change is a legal-structure one, the remaining engineering facts, and one correction to a source citation Cybersol had made itself. In summary — **§9.4** is rewritten as a single section, taking counsel's own wording for non-material revisions and a 30-day advance-notice mechanism (termination without liability plus pro-rata refund, prior version governing until the effective date, continued use thereafter constituting acceptance) for material ones, with hard-gate re-acceptance reserved for changes lacking a compliant Article 28(3) basis; **§8.2's** confidentiality carve-out is struck on counsel's recommendation, leaving wilful misconduct or gross negligence; **§8.3** folds in the two counsel questions now answered and marks the third as still open; **§4(a)** and **§4(c)** record that vendor-side abuse monitoring falls outside Cybersol's documented instructions and set out how Annex 2 may be revised; **§6.1** discloses that an individual engaged by Cybersol accesses production systems from outside the EEA, **without pre-judging how that access is classified**, and narrows the filename disclosure now that the deployed build is established; **§6.2** records that the addendum's 2021 Standard Contractual Clauses are a processor-to-processor module between two Microsoft entities and therefore do **not** cover the Cybersol-to-Microsoft path; **§5.2** names email to the account's administrative address as the promised notice channel; **§4(g)**, Annex 1 and the Annex 2 backups row correct the retention position to bounded 30-to-35-day storage cycles, which supersedes the 5 August 2026 statement that nothing pruned either backup leg and corrects a recoverability claim that had been wrong in the direction that overstates recoverability; Annex 2 refreshes the evidence-chain figure to 13/13, moves the legacy-record purge into the past tense, and restates vulnerability scanning as CI-integrated while disclosing an August 2026 interruption; the **no-training** row now cites the vendor addendum directly rather than an internal draft proposal, states the edition as the worldwide English edition last updated 1 September 2025, and asks reviewers to assess whether model training falls within the addendum's purpose limitation rather than presenting that as settled; the **abuse-monitoring** row adds the vendor's independent-controller role, its representative entity, the human-access fact, and the retention limitation as a disclosed limitation rather than a figure; and **Annex 3** records the Google Workspace contracting entity and region posture while leaving its Chapter V status expressly contested. **No PDF has been generated from this or any intervening revision.** All of it reaches counsel only inside the single consolidated version, diffed against the v10 he then held.*

*Review draft v10 — 10 August 2026 (Annex 2 no-training basis restated. **This is a change of substance and it supersedes what v9 told you.** The v9 row asserted that the AI sub-processor's undertaking not to train on Customer data was a contractual commitment under its service terms. On review of the governing data-protection addendum — the worldwide English edition, last updated **1 September 2025** (an earlier statement of this header cited an edition of 22 May 2026; that citation is withdrawn on the strength of the document's own header, and whether an edition of that date exists in another language is an inference this document does not draw) — **no clause in it names model training**, which Cybersol has since verified by searching the whole document rather than inferring it. The undertaking is therefore restated on the basis actually available: the addendum's **general purpose limitation** — Customer Data may be processed only for the enumerated purposes or on the Customer's documented instructions — together with the vendor's **published product documentation**, which states that prompts and completions are not used to train, retrain or improve the base models (reviewed 7 August 2026). The factual position is unchanged — no training on Customer Data occurs — but the **legal basis relied on is narrower than v9 represented**, and reviewers are asked to assess the sufficiency of a purpose-limitation-plus-vendor-documentation basis rather than of a named contractual no-training clause. No other row is changed. **v9 of 7 August 2026 is the copy sent to ICTRecht on 7 August 2026; v10 supersedes it and is the copy to review.**) — prior header: Review draft v9 — 7 August 2026 (§4(g) text-integrity correction, no change of substance: a bracketed internal verification marker survived the de-marking pass into v8 and appeared in the sentence disclosing backup-retention mechanics. Removing it also repairs the sentence it had broken — the trailing clause "during which they remain access-controlled and are not processed for any other purpose" had lost the*

antecedent it once attached to, so the assurance now reads “For as long as such backup copies persist, they remain access-controlled and are not processed for any other purpose.” **The backup-retention disclosure itself is unchanged:** the retention target is still stated as defined-but-not-achieved as of 2026-08-05, and the access-control assurance is preserved, not weakened. Note that v8’s own header asserted “no bracketed verification markers remain in this copy” — that assertion was untrue of v8 and is true of v9. **v8 of 6 August 2026 is the copy sent to ICTRecht on 7 August 2026; v9 supersedes it and is the copy to review.**) — prior header: Review draft v8 — 6 August 2026 (customer-managed-key correction: the Annex 2 row previously described the planned option as giving “independent cryptographic revocation of Cybersol access”; on the design of record the backend would hold a standing decrypt permission, so the row now states custody and prospective revocation and is expressly not counted as a supplementary measure. §6.2 now enumerates the measures relied on, which it previously incorporated by wholesale reference to Annex 2. **v6 of 3 August 2026 is the copy sent to ICTRecht; v7 of 5 August was never sent. v8 supersedes both and is the copy to review.**) — prior header: Review draft v7 — 5 August 2026 (backup-retention and database-role truth-alignment pass; supersedes v6 of 3 August 2026, which was the change-management layer over v5). **v6 was the copy sent to ICTRecht on 2026-08-03; this v7 differs from it in four places — §4(g) deletion mechanics, Annex 1 Duration, Annex 2 Backups, Annex 2 Tenant isolation — so the two must not be treated as the same instrument.** Prepared for external legal review; supersedes and replaces the 27 July 2026 draft in full. Statements carrying an in-line date reflect verification against the production environment as of that date; undated statements are sourced from Cybersol’s governance record and are re-verified before issuance. Facts still requiring verification at issuance are stated in prose with a dated qualification; no bracketed verification markers remain in this copy. Not an executed operative DPA.

Processor: Cybersol B.V. **Platform:** OBLIGO (a product brand of Cybersol B.V. — not a separate legal entity).

Parties

This Data Processing Agreement (“**DPA**”) forms part of, and is incorporated by reference into, the commercial agreement between the Customer and Cybersol governing the Customer’s use of the OBLIGO platform (the “**Agreement**”).

- **Cybersol B.V.**, a private limited liability company (*besloten vennootschap met beperkte aansprakelijkheid*) incorporated under the laws of the Netherlands, registered with the Kamer van Koophandel under number **70016348**, RSIN **858104957**, statutory seat (statutaire zetel) in **Amsterdam**, visiting/operational address Wilhelmina van Pruisenweg 104, HSD Campus, 2595 AN ’s-Gravenhage (The Hague) (“**Processor**”, “**Cybersol**”), represented for acceptance by its sole and independently authorised director (per the Chamber of Commerce register); and
- the **Customer**, being the legal entity identified as the Customer under the Agreement when this DPA is accepted or concluded under §9 (“**Controller**”, “**Customer**”); another legal entity recorded in the same OBLIGO workspace does not thereby become a party to this DPA.

“OBLIGO” is the trading name under which Cybersol B.V. operates the platform; Cybersol B.V. is the sole contracting legal entity.

1. Definitions

Terms “personal data”, “processing”, “controller”, “processor”, “data subject”, “sub-processor”, “personal data breach”, “special categories of personal data” have their GDPR (Regulation (EU) 2016/679) meanings.

- “**Customer Personal Data**” — personal data in the contracts, documents and records the Customer

submits to the OBLIGO platform, and personal data generated by OBLIGO's processing of that content (AI-extracted obligation records + metadata), processed by Cybersol on the Customer's behalf under this DPA. - "**Services**" — the OBLIGO contract-obligation-management SaaS platform. - "**SCCs**" — the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914.

2. Roles and scope

2.1 For Customer Personal Data, the Customer is the **Controller** and Cybersol is the **Processor**, processing solely to provide the Services and only on the Customer's documented instructions (§4(a), Annex 1). **2.2** For account, authentication, billing and platform-operation data about the Customer's users, Cybersol acts as an **independent controller** under its own Article 6 basis and Privacy Notice; that processing (including payment processing via Stripe — see Annex 3 note) is outside this DPA. **2.3** This DPA must be validly accepted **before** Cybersol first ingests Customer contract content (Art 28(3) chapeau: processing "shall be governed by a contract"). (retrieved: <https://gdpr-info.eu/art-28-gdpr/>, 2026-07-27.)

2A. Controller obligations and rights

2A.1 Controller obligations / warranties. The Customer warrants and undertakes that: (a) it has a valid lawful basis under Articles 6 (and, where applicable, 9 and 10) GDPR for the Customer Personal Data it submits and for its processing by Cybersol under this DPA; (b) its instructions to Cybersol (including its configured use of the Services) are lawful and will not put Cybersol in breach of the GDPR; (c) as between the Parties, it is responsible for the lawfulness of the content it submits, **including any special-category data (Art 9) or criminal-offence data (Art 10) it chooses to upload** — Cybersol does not solicit, require, or screen for such data before ingestion — and for providing any notices to, and obtaining any consents from, data subjects that its own controller obligations require; this allocation does not relieve Cybersol of its own obligations as processor under this DPA and the GDPR; (d) it will not use the Services to process personal data for which it lacks controller authority. **2A.2 Controller rights.** The Customer has the right to: give and amend documented instructions (§4(a)); receive notice of and object to sub-processor changes (§5.2); request compliance information and audits (§4(h)); receive breach notifications (§7); and elect return or deletion of Customer Personal Data (§4(g)). This §2A satisfies the "obligations and rights of the controller" particular of the Article 28(3) chapeau; see also Annex 1.

3. Subject-matter, duration, nature, purpose, data

Set out in **Annex 1**. Duration: the subscription term + the §4(g) return/deletion period.

4. Processor obligations (Article 28(3)(a)–(h) GDPR)

Cybersol shall: **(a) Documented instructions.** Process Customer Personal Data only on the Customer's documented instructions (this DPA, the Agreement, and configured use), including as to third-country/international-organisation transfers, unless required by Union/Member-State law — in which case Cybersol informs the Customer before processing unless the law prohibits it on important public-interest grounds. Cybersol immediately informs the Customer if, in its opinion, an instruction infringes the GDPR or other Union or Member-State data-protection provisions. (Art 28(3)(a) + final subparagraph.) **Vendor-side abuse monitoring falls outside these documented instructions.** The AI sub-processor's abuse monitoring, described in the Annex 2 abuse-monitoring row, is carried out by that sub-processor as an independent controller for its own purposes. It is therefore not processing on the Customer's documented instructions under this paragraph, and no Customer instruction or acknowledgement is sought for it; the Annex 2 row is the disclosure, not an instruction. **(b) Confidentiality.** Ensure persons authorised to process are bound by confidentiality or a statutory duty. (Art 28(3)(b).) **(c) Security.** Implement the Article 32

measures in **Annex 2. (Art 28(3)(c).)** Cybersol may update the technical and organisational measures in Annex 2 to reflect changes in technology, implementation or security practice, provided that the updated measures do not materially reduce the protection of Customer Personal Data or the Customer's rights under this DPA; in assessing an update, Cybersol considers the nature, scope, context and purposes of the processing and the risks addressed by the affected control. An update does not cure or remove a limitation or open item expressly disclosed in Annex 2 unless the revised Annex identifies the evidence and date on which its resolution was verified. Updates that materially reduce protection, or that amend another substantive term of this DPA, require agreement in accordance with §9.4. Each revision of Annex 2 is published as a dated version with version history and a change log, and is notified to the Customer through the §10 notice channel; and Cybersol records its no-material-reduction assessment for each revision — who assessed it, against which control, and on what date. The publication and notice commitments bind on issuance; the internal assessment record is not yet built, and that is disclosed rather than assumed. **(d)**

Sub-processors. Engage sub-processors only per §5. *(Art 28(3)(d).)* **(e) Data-subject rights.** Taking account of the nature of processing, assist the Customer by appropriate technical/organisational measures, insofar as possible, to respond to Chapter III data-subject requests. *(Art 28(3)(e).)* **(f) Compliance assistance.** Assist the Customer, taking account of the nature of processing and information available to Cybersol, with Articles 32–36 (security, breach notification, DPIAs, prior consultation). *(Art 28(3)(f).)* Cybersol will make available its then-current system-level DPIA support materials for the OBLIGO contract-processing path when it is complete. **(g) Return or deletion.** At the Customer's election, **made at any time before or within 30 days after the end of the provision of the Services**, delete or return all Customer Personal Data and delete existing copies, unless Union/Member-State law requires retention. If the Customer makes no election within that window, Cybersol deletes all Customer Personal Data within a further 30 days. Return of obligation records and document metadata is available self-serve (structured JSON, encrypted archive; rate-limited) at no additional fee; contract file bodies are returned on request as part of a §4(g) election. Deletion mechanics, disclosed: deletion is effected in the live production environment within the stated period; copies held in backup media are not individually erasable. **Lifecycle policies delete them after 30 to 35 days**, measured on 18 August 2026 against the live lifecycle policies of the production storage account: the container holding the hourly and nightly logical snapshots at 35 days, the write-ahead-log archive at 30 days, and the base-backup archive at 35 days; all three policies enabled and all predating 4 August 2026. **Blob soft delete is also enabled for the backup storage, with a 30-day retention period** (recorded on 4–5 August 2026 and restated on 4 October 2026), so a copy deleted by a lifecycle policy remains in a soft-deleted, recoverable state for up to that further period before it is permanently removed. These periods describe the configured cycles; they are not a guarantee that every copy is permanently removed by a particular date. The point-in-time-recovery window is correspondingly bounded. **This supersedes what this clause stated as of 5 August 2026** — that no deletion mechanism removed copies from either backup leg, so copies were retained from the point each leg began. That earlier statement was established from Cybersol's own application code and runbooks, which hold no infrastructure-as-code for the backup storage account, and it disclosed at the time that whether an out-of-band storage-lifecycle policy prunes either container was not established from that record. It is now established, and it does: the pruning is performed by the storage platform, out of band from the application, which is why a code-and-runbook reading could not see it. The approximately 14-day figure carried in earlier revisions of the Annex 2 backup rows was a target that was never implemented, and is superseded by the measured cycles above rather than merely doubted. For as long as such backup copies persist, they remain access-controlled and are not processed for any other purpose. Evidence-Locker audit records are retained for up to 7 years for the audit-trail function. On erasure of the underlying data they are amended: identifiers and recognised personal-data fields are anonymised. As an open item, disclosed here, excerpts held in other fields of those records survive that amendment; their removal is an open remediation item and will be recorded in a dated revision once verified. This disclosure does not permit customer content to be retained for that period, does not excuse that open item, and does not replace its remediation and verification; the deletion obligations in this §4(g) are unchanged. **(h) Audits — see §4(h) below.**

§4(h) Audit clause. Cybersol shall, on reasonable written request, make available the information necessary to demonstrate compliance with Article 28 GDPR and this DPA, and shall allow for and contribute to audits, including inspections, conducted by the Customer or an auditor it mandates, in accordance with Article 28(3)(h) GDPR. The Parties agree the following **operational framework** (which allocates method, frequency and cost but does not remove the Customer's underlying right): (1)

Documentation first (normal method). Cybersol will provide, on request: its most recent third-party audit report(s)/certification(s) covering the processing (including, once obtained, ISO/IEC 27001 or a SOC 2 Type II report — Annex 2 for current status); written responses to a reasonable standard-form security questionnaire; and a current summary of the Annex 2 measures. (2) **On-site / remote audit.** Where the Customer **reasonably considers** the documentation in (1) insufficient to verify a specific and legitimate audit requirement (including one imposed on the Customer by its own regulator), the Customer, or a reputable non-competitor third-party auditor it mandates (bound by confidentiality no less protective than this DPA), may conduct an audit or inspection, subject to: (A) **≥ 30 days'** prior written notice; (B) scope reasonably limited to Cybersol's processing of that Customer's own Customer Personal Data and the Annex 2 measures; (C) Cybersol's normal business hours, minimising disruption and protecting other customers' data confidentiality; (D) the Customer bearing its own and Cybersol's reasonable participation costs, **except** where the audit finds a material Cybersol breach of this DPA, where Cybersol bears its own costs; (E) a mutual NDA, which Cybersol shall promptly execute on reasonable standard terms, before on-site access. Frequency is **once per rolling 12-month period** except where a supervisory authority requires more, following a personal data breach affecting the Customer, or to verify remediation of a material finding from a prior audit. (3) Cybersol may withhold access to another customer's data, its trade secrets, or confidential information not reasonably necessary to the audit's stated purpose. (4) Nothing here limits a supervisory authority's Article 58(1) powers (which proceed under its own authority, free of the notice/frequency/cost conditions above), nor Cybersol's breach-cooperation duty under §7. *(Drafting note: the documentation-first / frequency / cost terms reflect negotiated market practice, not the Article 28(3)(h) statutory floor; the base right to audit where the Customer reasonably requires verification is preserved.)*

5. Sub-processors (Article 28(2) and (4) GDPR)

5.1 The Customer gives **general written authorisation** for Cybersol to engage the sub-processors in **Annex 3**. **5.2** Cybersol gives **≥ 30 days'** prior notice of any intended addition/replacement. Notice is given **by email to the administrative email address registered on the Customer's account** (the §10 address); Cybersol may additionally publish the change on a public page, but the email is the promised channel and a published page is not relied on as notice. The purpose of that notice is to let the Customer object on reasonable data-protection grounds. Where an existing sub-processor's own change notice to Cybersol is shorter than 30 days, Cybersol passes the notice to the Customer without undue delay and the objection period runs from that notice. If the Customer objects within that period and the Parties cannot resolve it in good faith within a further 30 days, the Customer's remedy is to terminate the affected Services without further liability for that termination; fees already accrued are unaffected, and prepaid fees attributable to the unused period after the termination date are refunded pro-rata. **5.3** Cybersol imposes, by written contract, data-protection obligations the same in substance as this DPA on each sub-processor (including an Article 46 mechanism for any non-EU/EEA sub-processor without adequacy, per §6), and remains fully liable to the Customer for each sub-processor's performance. *(Art 28(4).)* **Stated exception (as of 10 August 2026):** this undertaking holds for every Annex 3 entry except the **Google Workspace** row, whose applicable written terms are **not yet established (as of 10 August 2026)**; it was added to Annex 3 with that status disclosed rather than held back.

6. International transfers

6.1 Customer contract content, and the obligation records derived from it, are processed within the **EU/EEA** — Azure swedencentral, backup geo-pair sweden-south (production configuration measured 2026-07-31); Cybersol does not, by platform design, route contract content through infrastructure outside the EU/EEA. Transactional-email delivery uses a US-based sub-processor (Annex 3): recipient name, email address and delivery metadata are processed in the United States under the EU SCCs and that sub-processor's EU-US Data Privacy Framework certification. **Clause and obligation text is not transmitted** to that sub-processor — notification templates render identifiers and metadata rather than contract prose, with a fail-closed sensitive-content validator as a developer-error backstop. Disclosed limits of that boundary: uploaded-file **names** (which can reveal a counterparty or contract title) and user-typed free text in support messages can transit the email leg, and this agreement continues to disclose them on that basis. A change reducing the filename exposure has been made in Cybersol's codebase and verified there on 17 August 2026: the malware-rejection notice carries no filename in its subject and, in its body, only a masked descriptor — the length of the name and its file extension — rather than the name itself. **That verification is now complete, so the disclosure narrows.** Production runs a single sealed release, verified on 18 August 2026, which contains both the masking change of 6 August 2026 and its hardening of 11 August 2026, so the masking behaviour is what production runs and file names are **not** transmitted on the malware-rejection notice. The free-text limb is unchanged: support messages a user types are transmitted as written. Customer contract **bodies** remain within the EU/EEA. **Access from outside the EEA, disclosed.** An individual engaged by Cybersol to build and operate the platform accesses production systems, and therefore Customer Personal Data, **from outside the EEA.** That access has been classified on external counsel's advice (received September 2026): the individual is a **sub-processor within the meaning of Article 28(2)–(4)**, the applicable transfer instrument is **Module 3 of the 2021 Standard Contractual Clauses**, and §5.3 is the operative provision. **Status as at 9 September 2026, disclosed:** no separate binding data-protection agreement and no executed Standard Contractual Clauses have been concluded between Cybersol and that individual; the written contract §5.3 requires and the Article 46 mechanism §6 requires have not been concluded, and §5.3 and §6.3 are not qualified by this disclosure. As at the same date no Customer Personal Data has been processed under this agreement, no external customer, subscriber or tester having been admitted. **6.2** Cybersol's position is that its cloud sub-processor, Microsoft Ireland Operations Limited, is EU-established (Ireland) and processes within the EU per §6.1 — a characterisation put to counsel for confirmation, not asserted here as settled. Where a disclosure to a sub-processor — or that sub-processor's authorised remote access or onward disclosure — constitutes a transfer within the meaning of Chapter V GDPR without an adequacy decision, Cybersol will ensure the relevant transfer path is covered by an Article 46 mechanism (ordinarily the SCCs, Decision (EU) 2021/914, in the module matching the parties' roles for that path) **before the transfer occurs**, together with the Annex 2 supplementary measures relied on for this purpose — **per-tenant data-encryption-key envelope encryption and key-vault staff-decrypt isolation; no other Annex 2 row is relied on as a supplementary measure** — and a transfer impact assessment per EDPB Recommendations 01/2020, a summary of which Cybersol will make available on reasonable request once completed for the identified transfer path. As a precautionary posture — and because the question whether processing by an EU-established sub-processor with a US parent constitutes a Chapter V transfer at all is genuinely unsettled — Cybersol's adopted position is to incorporate the SCCs defensively even where the Chapter V trigger is contested; **the operative SCC module and addendum edition have now been established, and the answer does not reach this leg.** Measured against the governing addendum (worldwide English, last updated 1 September 2025), the instrument defines its 2021 Standard Contractual Clauses as *"the standard data protection clauses (processor-to-processor module) between Microsoft Ireland Operations Limited and Microsoft Corporation for the transfer of personal data from processors in the EEA to processors established in third countries which do not ensure an adequate level of data protection ..."*. The module is therefore processor-to-processor, and **the parties to it are two Microsoft entities:** those

clauses cover Microsoft's own onward transfer, not the Cybersol-to-Microsoft path this section concerns. Cybersol records that plainly rather than presenting the answer as covering its own leg, which it does not. *(This characterisation is one of the scoped review points.)* **6.3** For any future sub-processor whose engagement would involve **a transfer to a third country or international organisation within the meaning of Chapter V GDPR** without an Article 45 adequacy decision, Cybersol will put an Article 46 mechanism (ordinarily the SCCs) + a TIA + any necessary supplementary measures in place **before** the transfer and before that sub-processor is added to Annex 3. **Stated exception (as of 10 August 2026):** the **Google Workspace** row was added to Annex 3 while its transfer status is **not yet established (as of 10 August 2026)** and whether it involves a Chapter V transfer at all is contested; this sequencing undertaking is qualified for that row and holds unqualified for every other Annex 3 entry.

6.4 *(Transitional — added 9 September 2026; removed by a non-material revision under §9.4(b) once the arrangement is concluded and recorded.)* The individual contractor listed in Annex 3 is engaged from outside the EEA. As at 9 September 2026 the written contract §5.3 requires and the Article 46 mechanism §6 requires have not been concluded with that individual, and no Customer Personal Data has been processed under this agreement. Cybersol **will conclude both, and complete the transfer impact assessment, before any Customer Personal Data is transferred to or made accessible to that individual**, and does not treat this section or any disclosure in this agreement as a substitute for them. **This section qualifies neither §5.3 nor §6.3: their undertakings, and §6.3's timing, apply to that individual unchanged**; it records the present status and Cybersol's commitment, nothing less.

7. Personal data breach

Cybersol notifies the Customer **without undue delay** after becoming aware of a personal data breach affecting Customer Personal Data (*Art 33(2), verbatim: "The processor shall notify the controller without undue delay after becoming aware of a personal data breach."* — retrieved <https://gdpr-info.eu/art-33-gdpr/>, 2026-07-27), with the information reasonably available at the time that the Customer needs for its Articles 33/34 obligations, and further information as it becomes available.

8. Liability

8.1 Nothing here limits either Party's liability to data subjects or a supervisory authority under Articles 82/83 GDPR. **8.2** As between the Parties, each Party's aggregate liability arising out of this DPA is subject to the limitations and exclusions of liability in the **OBLIGO Terms of Service** forming part of the Agreement, and only while a version of those Terms is validly in force and incorporated in the Agreement. Carve-outs from any such cap are limited to wilful misconduct or gross negligence. The liability cap in those Terms, subject to those carve-outs, also applies to claims between the Parties for recourse or indemnity relating to compensation paid to data subjects under Article 82 GDPR, to the extent mandatory law allows; whether any exclusion of liability referred to in the first sentence applies to those claims is not determined by this §8.2, and §8.1 is unaffected. **8.3 Liability cap.** *(Drafting note for review — this is one of the scoped review points.)* The intended cap is **the greater of (a) the Customer's trailing-12-month fees, or (b) a €10,000 floor**, to be established in the **OBLIGO Terms of Service (clause 13), operative only while a version of them is validly in force and incorporated in the Agreement**, with §8.2 cross-referencing that ToS cap. *(Three questions were put for review. All three have now been answered; parts of (iii) remain open. (i) Incorporation under BW 6:233(b)/6:234, including storable, reproducible form at or before acceptance per BW 6:234(2)–(3) — answered, and the answer is a build instruction rather than a drafting one: the acceptance flow is to be built to the full standard for every customer, because Cybersol cannot see at self-serve sign-up which side of the BW 6:235(1) line a customer falls on. (ii) Substantive defensibility of the €10,000 floor under BW 6:233(a) for small-B2B customers, noting BW 6:235(1) — answered: a larger counterparty is excluded by 6:235(1) and cannot invoke 6:233 or 6:234 at all, so cannot attack the cap or its*

incorporation on those grounds; a mid-sized business customer can invoke 6:233(a) but faces a high bar. The assessment is favourable, and the cap is **not** thereby declared enforceable; BW 6:248(2) reasonableness is retained by everyone. (iii) Interaction with Article 82(5) GDPR recourse between controller and processor — **counsel's view received:** the Parties may agree their internal allocation, and the cap should state that it covers recourse and indemnity claims relating to Article 82 compensation; §8.2 now says so. This is a drafting decision, not legal clearance; whether the allocation operates one way or reciprocally, and how it fits the indirect-loss clarification in the Terms, remain open for legal validation.) Current state, disclosed (2026-08-03): self-serve customers today accept a platform-use disclaimer hash and the versioned pre-launch admission terms hash (§9.1) — Stripe Checkout is a card-capture step (setup mode), not an acceptance instrument, and does not record agreement to any terms. The pre-launch terms (v1.1) carry no liability cap. So no ToS liability cap is yet in force and §8.2 is inoperative until the ToS goes live; until then self-serve exposure is uncapped as between the Parties. The €10,000 floor is a deliberate startup-stage choice; enterprise buyers may negotiate a higher per-deal cap. Article 82/83 exposure to data subjects and regulators is uncapped by law regardless (§8.1). **8.4** This DPA takes effect on electronic acceptance (§9) and continues while Cybersol processes Customer Personal Data, notwithstanding expiry/termination of the Agreement, until processing ends per §4(g). **8.5** Governed by the laws of the Netherlands; the Parties submit to the exclusive jurisdiction of the competent court in **The Hague** (Rechtbank Den Haag), without prejudice to mandatory GDPR jurisdiction.

9. Acceptance (Article 28(9) — electronic form)

9.1 This DPA is **to be** accepted electronically by the Customer at its first access to the Services after approval of its application, and in any case before normal use of the Services begins. *(The DPA-specific electronic acceptance surface is not yet deployed — sign-up today records a platform-use disclaimer hash and a pre-launch-terms hash; the §9 mechanism is to be implemented before external customer onboarding, and the clauses below describe how it will operate once live.)* Article 28(9): “The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.” (retrieved <https://gdpr-info.eu/art-28-gdpr/>, 2026-07-27.) The Parties intend acceptance under this §9 to constitute a contract in writing, including in electronic form, for Article 28(9) purposes; on the Dutch-law formation basis, Cybersol's counsel advised on 14 August 2026 that contract formation is form-free (Articles 6:217 and 3:37 of the Dutch Civil Code), that click acceptance is a valid mode of formation provided the click is requested before the contract is concluded, and that Article 28(9) does not require a signature; counsel recommended designing the acceptance flow to the four safeguards of Article 6:227a of the Dutch Civil Code — accessibility of the agreement to the parties (for example, that it can be saved as a PDF), authenticity, the moment of formation, and the identity of the parties. That advice is not proof that the acceptance mechanism meets those safeguards: the mechanism is not yet deployed (see above), and whether it meets them is to be established when it is built. *(For completeness: even if the acceptance were characterised as an electronic signature, eIDAS (Reg. (EU) 910/2014) Art 25(1) would not deny it legal effect solely for being electronic — but eIDAS is not the primary basis for ordinary clickwrap formation here.)* **9.2** The individual accepting online, or the signatory of a written instrument under §9.5, represents and warrants that they are authorised to bind the Customer, and expressly confirms that authority when accepting or signing. Cybersol does not independently verify this. **9.3** Once the acceptance mechanism is deployed, Cybersol **will record** per acceptance: the Customer legal-entity name; DPA version + content-hash; timestamp; accepting user; reasonably available session context (IP, user agent). Retained for the Agreement term + any limitation period; reproducible to both Parties. **9.4** A revision that (a) refreshes dated implementation evidence in the Annexes, or (b) records the verified resolution of a limitation or open item previously disclosed in this DPA or its Annexes, identifying the evidence and the date of verification, and that in either case does not reduce the protection of Customer Personal Data or the Customer's rights under this DPA, is a non-material revision. Non-material revisions are published as dated versions with version history and are notified to the Customer, and do not require re-acceptance. A **material** revision is

announced to the Customer **at least 30 days before its effective date**. Before that date the Customer may terminate the affected Services without liability for the termination and with a pro-rata refund of prepaid fees for the unused period, mirroring the remedy §5.2 provides for sub-processor objections. The previously accepted version continues to govern until the effective date; from the effective date the new version applies to Customers that have not terminated, and continued use of the Services after that date constitutes acceptance of it. **Express re-acceptance operating as a hard gate — processing pausing until the new version is accepted — is reserved** for changes so fundamental that continued processing without acceptance would lack a compliant Article 28(3) basis, such as a change to the purposes of processing. **9.5** Pending deployment of the electronic acceptance surface, this DPA may equally be concluded by the Customer's execution of an order form, quotation, or other written instrument (including email confirmation) that identifies the Customer and this DPA by version and incorporates this DPA by reference, and in which the signatory expressly confirms their authority under §9.2.

10. Notices

Formal notices under this DPA — sub-processor objections (§5.2), return/deletion elections (§4(g)), audit requests (§4(h)), and breach-related communications (§7) — are given in writing: to Cybersol at legal@obligo.tech (confirmed 2026-08-03 — an existing alias of support@obligo.tech. **Corrected 17 August 2026: the previous wording reversed the two addresses.** As verified in the OBLIGO website source on 17 August 2026, legal@obligo.tech is the contact address given on all four OBLIGO legal pages — privacy, terms, cookies and data-processing — in each of the site's three languages; support@obligo.tech is given on the pricing and contact pages, and on no legal page. That verification is now complete: production runs a single sealed release, verified on 18 August 2026, which carries the locale files verified above, so the addresses stated here are the addresses the deployed site serves.), and to the Customer at the administrative email address registered on the Customer's account. Breach notifications under §7 may additionally be surfaced in-platform.

Annex 1 — Details of processing (Article 28(3) chapeau)

Field	Detail
Subject-matter	Processing of personal data in Customer-provided contracts/documents, to provide obligation-management via OBLIGO.
Duration	Subscription term + up to 60 days after the end of the Services for live-environment deletion (§4(g): a 30-day election window, plus a further 30 days for deletion if the Customer makes no election); thereafter, backup copies are governed by the backup-retention terms of §4(g), which is the operative home for backup-retention periods and which discloses that lifecycle policies delete those copies after 30 to 35 days (measured 18 August 2026) and that a deleted copy then remains recoverable under the backup storage's 30-day blob soft delete before it is permanently removed, superseding the position §4(g) stated as of 5 August 2026; and Evidence-Locker audit records persist, in amended form, for up to 7 years — both per §4(g).
Nature and purpose	Ingestion/storage of uploaded documents; AI-assisted clause/obligation extraction (with mandatory human review before any obligation becomes operational); obligation lifecycle management; notification support; Evidence-Locker audit-trail retention — only per §2.1/§4(a) instructions.

Field	Detail
Types of personal data	As in Customer-uploaded documents — typically names, business contact details, roles/titles, signatory info of counterparties, employees, and referenced individuals. The Customer controls content and may incidentally upload Article 9 special-category or Article 10 data; Cybersol does not solicit, require, or screen for it.
Categories of data subjects	The Customer's counterparties, signatories, and named individuals in submitted documents; and Customer personnel whose activity is reflected in Customer Personal Data (distinct from §2.2 account data).
Controller obligations & rights	Per §2A (lawful-basis and lawful-instruction warranties, responsibility for uploaded content incl. Art 9/10 data; rights to instruct, object to sub-processors, audit, receive breach notice, elect return/deletion).

Annex 2 — Technical and organisational measures (Article 32)

Dated measurements and implementation details in this Annex record the state verified on the stated date and were accurate to Cybersol's knowledge when recorded. They may be refreshed as technology and implementation change; such refreshes do not permit a material reduction in the protection required by this DPA (§4(c)). Contractual commitments, current implementation evidence, and disclosed open items are distinguished throughout.

Measure	Description	Status
Encryption in transit	TLS for client/server traffic at the public edge: the application gateway is pinned to a TLS 1.2 minimum with AEAD-only cipher suites (Azure predefined policy AppGwSslPolicy20220101S, applied 2026-07-31; verified externally — TLS 1.3 default negotiation, TLS 1.2 accepted, TLS 1.0/1.1 refused; port 80 is a permanent HTTPS redirect, no plaintext serving path).	In place at the public edge (measured 2026-07-31). Internal service-to-service transport is not separately evidenced and is not claimed here; it will be verified, and this row updated, before customer issuance.

Measure	Description	Status
Encryption at rest (app data)	Per-tenant DEK envelope encryption; each tenant DEK wrapped by a KEK in Azure Key Vault; one tenant's DEK compromise does not expose another's. Open item, disclosed (2026-08-03): an internal code review found that AI-extracted obligation evidence — the Evidence-Locker payload and per-obligation evidence-anchor records — is stored in plain (non-application-encrypted) fields; this appears to fall outside the DEK-envelope scope described here and is pending engineering verification.	In place for contract bodies and the fields confirmed DEK-encrypted; not yet confirmed for AI-extracted obligation evidence payloads (open item, pending engineering verification). The limited set of legacy records predating this control — 3 rows / 59,659 bytes in one cancelled tenant — was purged on 18 August 2026: 5 contracts and 5 contract files purged, 5 storage blobs deleted, no errors, and the oversized metadata count re-measured at zero. The forward commitment this row previously carried is discharged, and is stated in the past tense. Separately, and not cured by that purge, 481 obligation rows carry an evidence-anchor payload with no encrypted-field pointer (measured 18 August 2026); for those legacy rows the open item disclosed above remains accurate.
Key management / staff isolation	Per-tenant KEKs are held in Azure Key Vault. No human principal holds a Key Vault crypto role for tenant KEKs (verified 2026-07-31); decryption occurs only via the platform's managed service identity, and Key Vault data-plane audit logging is enabled (from 2026-07-31). Zero-visibility default for Cybersol staff; Tenant-Admin-granted, time-limited (4h), read-only, per-action-audited support access, revocable; Cybersol does not override tenant grants at the application layer (administrative-layer residual below). This is an organisational control, not a technical barrier: privileged administrative access could alter role assignments, and the same administrative access also reaches the credentials protecting the encrypted backup legs; technical prevention of administrator self-escalation (privileged-identity management, deny assignments, separate key custody) is not currently implemented and is a tracked hardening item. Keys are software-protected (standard SKU), not HSM-backed.	Organisational control in place; residual administrative access as disclosed; hardening tracked as a pre-launch item. Detailed privileged-access records are available under the §4(h) documentation/audit route.

Measure	Description	Status
Tenant isolation	tenant_id-scoped access; row-level security as defence-in-depth.	In place for tenant-content tables (row-level security enabled and forced by migration; verified in the codebase 2026-08-02). Qualifications: an audited, scoped administrative cross-tenant read path exists for operational use and, per a 2026-08-03 internal review, spans a substantial number of tables — re-measured 2026-08-05 as at least 22 distinct tables, applied across 16 migration files (the two are different units; the earlier “14 or more” was a table estimate now superseded). Static scan, migration order not replayed, so the figure is a floor rather than an exact count — its breadth is pending a scoping review; the same review found at least one auxiliary table (holding offboarding legal-hold state) with no row-level-security migration identified, also pending verification; database-role enforcement is in force in production — verified 2026-08-05 against the sealed production environment file and, re-measured 2026-08-18, across all nine running application containers; where the connecting role is a superuser or carries BYPASSRLS, the application refuses to serve rather than continuing. That control asserts the connecting role’s privileges; it does not by itself cure the qualifications noted above, nor the further conditions recorded under the same internal review, which are of a different kind.

Measure	Description	Status
Audit logging	Hash-chained Evidence Locker recording AI suggestions, human approve/reject, and security events; tenant chains cryptographically verified — 13/13 as of 2026-08-18, zero failures, across all thirteen tenants in every lifecycle state, superseding the earlier 9/9 figure, which covered a narrower population. Qualifications: retention/anonymisation functions can amend entries where required to satisfy Art 17 erasure (append-only in normal operation, not absolutely immutable); the chain digest is an unkeyed SHA-256 (internal-consistency verification, not tamper-evidence against database-level write access); the nightly verifier covers active/trial tenants only — two of the platform's six tenant-lifecycle states; suspended, cancelled and other dormant tenants are not covered by this nightly check (<i>corrects a prior "5 of 11 states" figure that did not match the platform's state model; corrected 2026-08-03; dormant-state coverage remains an open item</i>).	In place, with the qualifications noted.
AI data minimisation (extraction input vs. stored evidence)	The full contract document is sent to the EU-region AI sub-processor for extraction: production runs whole-document mode (verified in the production configuration across all nine running application containers, re-measured 2026-08-18), so the transient extraction input is the entire contract, not clause excerpts. Data-minimisation applies only at the stored-evidence layer: retained audit excerpts are length-capped (≤ 400 characters per obligation; full clause bodies are not persisted in the audit record).	Whole-document extraction input (measured); stored-evidence cap in place.

Measure	Description	Status
AI processing — no training	Extraction runs on the AI sub-processor's EU-region deployment; the sub-processor does not train on Customer data. The governing instrument is the Microsoft Products and Services Data Protection Addendum, worldwide English edition, last updated 1 September 2025; the edition is taken from that document's own header ("<i>Last updated September 1, 2025. Published in English on September 1, 2025.</i>"), and the copy relied on is held under hash so that what was read can be reproduced (SHA-256 b17d9bb8cf5bd87e9c7839f7e112bc5c8dcbaeb56f903abb560fb231b140a7a). That document contains no clause naming model training, and Cybersol verified this rather than assuming it: searched on 24 August 2026 across all 27 constituent parts of the document, the terms "OpenAI", "Azure OpenAI", "AI Services", "foundation model", "machine learning" and "abuse monitoring" each occur zero times, against control terms in the same pass that occur 85, 9 and 3 times respectively. The position therefore rests on the addendum's general purpose limitation, quoted here rather than characterised: "<i>When providing Products and Services, Microsoft will not use or otherwise process Customer Data, Professional Services Data, or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with Customer's documented instructions.</i>" Whether model training falls within that limitation is a legal reading; Cybersol does not make it itself, and records below counsel's answer on this addendum; that answer does not endorse any later wording. A separate "Processing for Business Operations" section of the same document authorises an enumerated list of purposes that includes "<i>product strategy</i>", bounded by processing "<i>without accessing or analyzing the content of Customer Data</i>". Cybersol reads the two sections as capable of pointing in different directions, reserves the question rather than resolving it internally, and has referred it for	In place. Basis: the addendum named above, plus vendor product documentation. (<i>Edition corrected 24 August 2026: this row previously cited an edition of 22 May 2026. That citation is withdrawn on the strength of the document's own header; whether an edition of that date exists in another language is an inference this agreement does not draw.</i>)

Measure	Description	Status
	external confirmation — reviewers are asked to assess that question rather than to accept a settled reading. Counsel's answer (September 2026): model training falls within the addendum's providing-section purpose limitation and is prohibited absent the customer's documented instructions; the Business Operations section authorises only aggregated statistics and metrics computed without access to or analysis of Customer Data content, and so excludes training by its own terms. Cybersol records that answer as counsel's reading; the edition cited above is unchanged. The factual position, that no training on Customer Data occurs, is separately supported by the vendor's published product documentation, which states that prompts and completions are not used to train, retrain or improve the base models (reviewed 7 August 2026). Models are stateless as to training.	

Measure	Description	Status
AI processing — abuse monitoring (disclosed default)	Who carries this out, and in what capacity. Modified abuse monitoring is not enabled on the subscription. Under the vendor's default, prompts and completions may be sampled and retained for abuse monitoring. The vendor carries out this processing as an independent controller for its own purposes, so it falls outside the documented instructions in §4(a), and §4(a) records the same boundary. The relevant vendor entity is Microsoft Ireland Operations Limited, which the governing addendum identifies as <i>"Microsoft's data protection representative for the European Economic Area and Switzerland"</i>, at One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland. That is the role the addendum gives it, and this row does not describe it as the processor for this processing, because for this processing it is not acting as one. Human access, stated plainly. Flagged prompts and completions <i>"can be accessed for human review only by authorized Microsoft employees via Secure Access Workstations (SAWs) with Just-In-Time (JIT) request approval granted by team managers"</i>, and <i>"For Models sold by Azure deployed in the European Economic Area, the authorized Microsoft employees are located in the European Economic Area."</i> The material fact is not how long flagged content is kept, but that a vendor employee may read it. Retention duration — sought, and not obtainable. Cybersol sought confirmation from Microsoft of the retention period applied when prompts and completions are sampled for abuse monitoring. On 22 August 2026 Cybersol checked the vendor's published abuse-monitoring and data-privacy documentation for the models used, the Limited Access documentation, the Code of Conduct for Microsoft AI Services, and the Microsoft Products and Services Data Protection Addendum (worldwide English, September 2025); none states a retention period for this processing, and the Addendum does not address this processing at all. Cybersol does not represent a retention duration and does not treat the absence of a stated period as evidence that it is short, long	Default abuse monitoring in effect; the opt-out was applied for on 25 August 2026 and refused by the vendor on 27 August 2026 (the option is open to managed-customer/partner accounts only; no re-application path exists at present). The default, and this row's disclosure of it, remain in effect (measured 2026-07-31; refusal recorded 27 August 2026). Arrangement last verified on 18 August 2026 against the production subscription: default abuse monitoring in effect — the production Azure OpenAI resource showed no modified-abuse-monitoring configuration or capability. Cybersol confirmed on 4 October 2026 that this arrangement remains in effect; that confirmation is not a new verification.

Measure	Description	Status
	or bounded. That retention-limitation statement carries its own correction triggers, in the vendor-supplied wording: This entry is corrected the first time the vendor states or confirms a period, and is removed only once modified abuse monitoring is in effect for Cybersol's subscription and that is verified, since that ends the storage this entry describes; a grant of the application does not by itself change this row. What a granted application would and would not change — stated once for this row. If the application is granted, the storage and the human review described above stop while the approval is in effect, and, once modified abuse monitoring is in effect and that is verified, the retention-limitation statement immediately above falls away with them, because it exists only to describe that storage. The rest of this row does not fall away. Automated review may still be conducted, so a grant narrows this row rather than retiring it. Under the present default, human review of flagged content is possible and is disclosed as such above; and a grant does not end abuse monitoring altogether. Given whole-document extraction (see the AI-data-minimisation row), the unit of any such retention is a full contract. Text for your own privacy notice is provided in Cybersol's sub-processor due-diligence pack, which is available on request. The honest gap: the vendor offers no contact route specific to this processing — the only form on either published page is the modified-monitoring application, and privacy questions route to the vendor's general privacy channel. This row says so rather than implying a channel that does not exist.	
Backup encryption (open pre-launch item)	The continuous WAL archive and the daily base backups are client-side-encrypted before leaving the DB host; but the hourly pg_dump snapshot is compressed, not app-layer-encrypted — reaches storage under provider-managed SSE only. This is a tracked pre-launch security item, to be closed before any external paying tenant is onboarded.	Open (pre-launch item)

Measure	Description	Status
Disaster recovery	Restore procedure exists (internal restore runbook) targeting ~30-min RTO. Not confirmed by a passing measured drill — the runbook itself states the RTO target has never been measured; the internal record classifies it as plausible but unverified.	Procedure documented; RTO target not drill-verified.
Backups (general)	Three legs: an hourly logical pg_dump snapshot, continuous WAL archiving (segment-based, 60-second forced switch; not streaming replication, no standby), and daily base backups. Backup storage is geo-redundant (Azure GRS, swedencentral → sweden-south; asynchronous, not a readable warm standby). Encryption posture per the Backup-encryption row above; backup deletion and retention are governed by §4(g), which is the operative home for retention periods and which discloses that lifecycle policies delete backup copies after 30 to 35 days (measured 18 August 2026) and that a deleted copy then remains recoverable under the backup storage's 30-day blob soft delete before it is permanently removed. Recoverability, disclosed: point-in-time recovery is bounded by those cycles — the write-ahead-log archive is retained 30 days and the base-backup archive 35 days, so recoverable history does not extend indefinitely and does not grow without limit. This row previously stated the opposite, that recoverable history extended back to the point continuous archiving began and grew daily; that statement was wrong in the direction that overstates recoverability, and is corrected here. The internal inconsistency this row carried against §4(g) is resolved by the same measurement. The previously stated approximately 14-day window was a target never implemented, and is superseded rather than merely doubted. Restore not yet drill-verified (see Disaster recovery).	Backups run as described; recoverability window + restore drill open.

Measure	Description	Status
Vulnerability management	Dependency and static-analysis scanning (pip-audit, Bandit) is integrated into continuous integration and gated on changed paths (verified 2026-08-18). Continuity is not claimed for the period 11 to 18 August 2026 , during which execution was interrupted by an exhausted continuous-integration plan quota; the interruption was remediated on 18 August 2026. Because scanning is gated on changed paths it is not a continuous scan of the whole estate, and none is claimed.	In place, path-gated; the August 2026 interruption is disclosed rather than smoothed over.
Customer-managed key	Tier 2+ customers may opt to hold, in their own cloud key-management account, the key-encryption key that wraps their tenant data-encryption key. On the design of record the OBLIGO backend would hold a standing decrypt permission on that key, so the option gives the customer key custody and the ability to revoke Cybersol's access prospectively — it does not make Cybersol unable to decrypt while the permission stands, and it is not offered as a defence against legal compulsion.	Not deployed; planned (Tier 2+); not counted as a supplementary measure.
Certifications	Cybersol B.V. holds no ISO/IEC 27001 or SOC 2 attestation today; both are roadmap targets and are not represented as current controls. The underlying cloud platform (Microsoft Azure) holds ISO 27001 and SOC 2 Type II within its own platform scope.	Roadmap; not current.

Annex 3 — Sub-processors

Sub-processors engaged to process **Customer Personal Data**:

Sub-processor	Role	Location
Microsoft Ireland Operations Limited (Microsoft Azure)	AI-assisted extraction and supplier-incident relevance tiebreaking — the tiebreak sends a counterparty legal-entity name and obligation metadata to the same deployment, with no clause text and no document body (verified in the codebase 2026-08-17); key management (Key Vault); document/DB/backup storage; compute hosting.	EU — Sweden Central (platform, storage, keys; backup geo-redundancy Sweden South; production configuration measured 2026-07-31). AI extraction runs on an EU Data Zone deployment — bounded to the EU geography, not pinned to a single region (also measured 2026-07-31).

Sub-processor	Role	Location
Plus Five Five, Inc. (d/b/a Resend)	Transactional email delivery (account notices, obligation reminders); data: recipient email address + name + message metadata, plus user-typed support text where a notification carries them. The filename limb has narrowed: per §6.1 the deployed build masks the name on the malware-rejection notice, so file names are not transmitted on that notice; the free-text limb is unchanged. No clause/obligation text — templates render identifiers and metadata rather than contract prose, with a fail-closed sensitive-content validator as a developer-error backstop — so contract bodies do not cross to this leg. Resend’s own sub-processors (hosting/sending) include Amazon Web Services (US); 14-day sub-processor change-notice.	United States — account data, metadata, and logs are stored in the US regardless of the sending-region selected (Resend GDPR page; DPA §6.1). Transfer basis: EU Standard Contractual Clauses (Commission Decision 2021/914) + Resend’s EU-US Data Privacy Framework certification. Verified 2026-08-03 against Resend’s published DPA (edition dated 2025-12-31; binding via ToS acceptance — no separately-executed PDF exists): US-processing/transfer at §6.1 as cited, SCCs at §§6.2–6.5, DPF commitment at §11; retention split — return-or-delete on service completion (§2.4), deletion within 90 days of account termination (Exhibit A).
Google Cloud EMEA Limited (Google Workspace — shared support mailbox)	Receipt and handling of in-product support requests and support-access requests: your user’s email address, the free text they type, the tenant name, the title and in-app address of the page the request was made from, and the request reference. Account, authentication and platform-operation mail about your users is not covered by this row — under §2.2 that processing sits with Cybersol as an independent controller, outside this agreement. No retention or storage-location representation is made, because none has been measured.	Contracting entity: Google Cloud EMEA Limited, 70 Sir John Rogerson’s Quay, Dublin 2, Ireland — the entity the vendor’s published rule assigns to a customer whose billing address is in the EMEA region other than France, Italy or Poland; Cybersol’s billing address is in the Netherlands, the account is purchased direct from the vendor with no reseller, and on a monthly billing cycle the current published terms are already operative for it. Data region: none is set. The vendor’s documentation records that the data-regions feature is included in this account’s edition, so its absence is an unexercised configuration choice rather than an edition limitation (vendor documentation reviewed 24 August 2026); because no data-region policy is configured, no commitment is made as to the country in which this data is processed — processing may occur in any country in which the vendor or its sub-processors maintain facilities. No retention or storage-behaviour representation is made, because none has been measured. The vendor’s Cloud Data Processing Addendum was accepted on 20 August 2026. Whether this destination involves a Chapter V transfer at all remains genuinely contested and is deliberately not resolved here, on the same footing as the Microsoft-Ireland position in §6.2.

Sub-processor	Role	Location
An individual contractor engaged by Cybersol (sole proprietor, Türkiye)	Development, deployment, debugging and operational support of the platform by remote access into the EU production environment (run-command into the EU host; application-UI sessions; support-access grants, used to date only in tests). Privileged infrastructure access. As at 9 September 2026: no external customer tenant exists and no Customer Personal Data has been processed under this agreement; access to date touched internal and test tenants only (the engineer's dated attestation of 9 September 2026). On his own dated attestation of 9 September 2026, the engineer has downloaded no blob, backup, database dump or log to his device outside the EEA; that is his account of his own actions, not an independently established download history. <i>Corrected by the engineer's dated statement of 4 October 2026, in his words:</i> "Correction to 9 September: on 8 July a production dump was downloaded for the recovery drill (no real customers then) and has been deleted." He also states: "No production database dump is stored." Tenant export archives — AES-encrypted archives created and stored on the EU production server, served through single-use, time-limited download links — are a distinct category: the download record identifies the user but does not carry the location, and whether other evidence can establish the location remains unresolved, so no statement is made about whether any export was, or was not, downloaded outside the EEA (the engineer's export-archive statement of 10 September 2026). Tooling residue of internal and synthetic tenants exists on that individual's encrypted device and, as session content, with the providers of the AI coding tools he uses (his attestation of 9 September and his tooling follow-up of 10 September 2026). Tooling used by that individual in the course of this access is under assessment as at 9 September 2026; this row neither lists nor excludes any further recipient on that account.	Türkiye (no adequacy decision). Classification: sub-processor, Art 28(4); instrument: 2021 SCCs, Module 3, to be annexed to the §5.3 written contract, with a transfer impact assessment. Status as at 9 September 2026: no separate binding data-protection agreement and no executed SCCs concluded; §5.3 and §6.3 are not qualified for this row.

Note on Stripe. Stripe Payments Europe, Limited processes payment/subscription/billing data, for which **Cybersol acts as an independent controller** (§2.2). Because that data falls outside the **Customer Personal Data** scoped by this DPA (§1 — contract/document content), Stripe is **not a sub-processor**

under this DPA, and its engagement is disclosed in Cybersol's Privacy Notice. This exclusion is a data-category scope point and does not purport to determine Stripe's own controller/processor status vis-à-vis Cybersol.

Annex 3 is versioned with this DPA. Additions or replacements of sub-processors are governed exclusively by §5.2, including its prior-notice and objection procedure, which this Annex's versioning does not limit. Cybersol retains prior versions of this Annex. The per-acceptance record — which DPA version and content hash each Customer accepted — is the record §9.3 provides for; as at 2026-08-17 it is not yet in operation, because the acceptance surface described in §9.1 is not deployed and no Customer has yet accepted this DPA.
